Fortinet Recommended Security Best Practices

Table of Contents

Version history

April 2017: V1.0
Initial security checks available with FortiOS 5.6.0

1 What is the Security Fabric?

The Security Fabric provides an intelligent architecture that interconnects discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire enterprise attack surface.

2 What is a Security Fabric Audit?

The Security Fabric gives a 360 degree continuous view of assets, networks and data movement within the organization. With dynamic business changes and increasing demand from on-net/off-net devices, IoT and other applications, organizations need a method to continuously monitor the effectiveness of their Security Fabric configuration.
The Security Fabric Audit and Scoring feature provides a method to continually take a pulse of the current security posture, and assess the effectiveness in managing security risks to critical networks and enterprise assets.

3 Why would I use this feature?

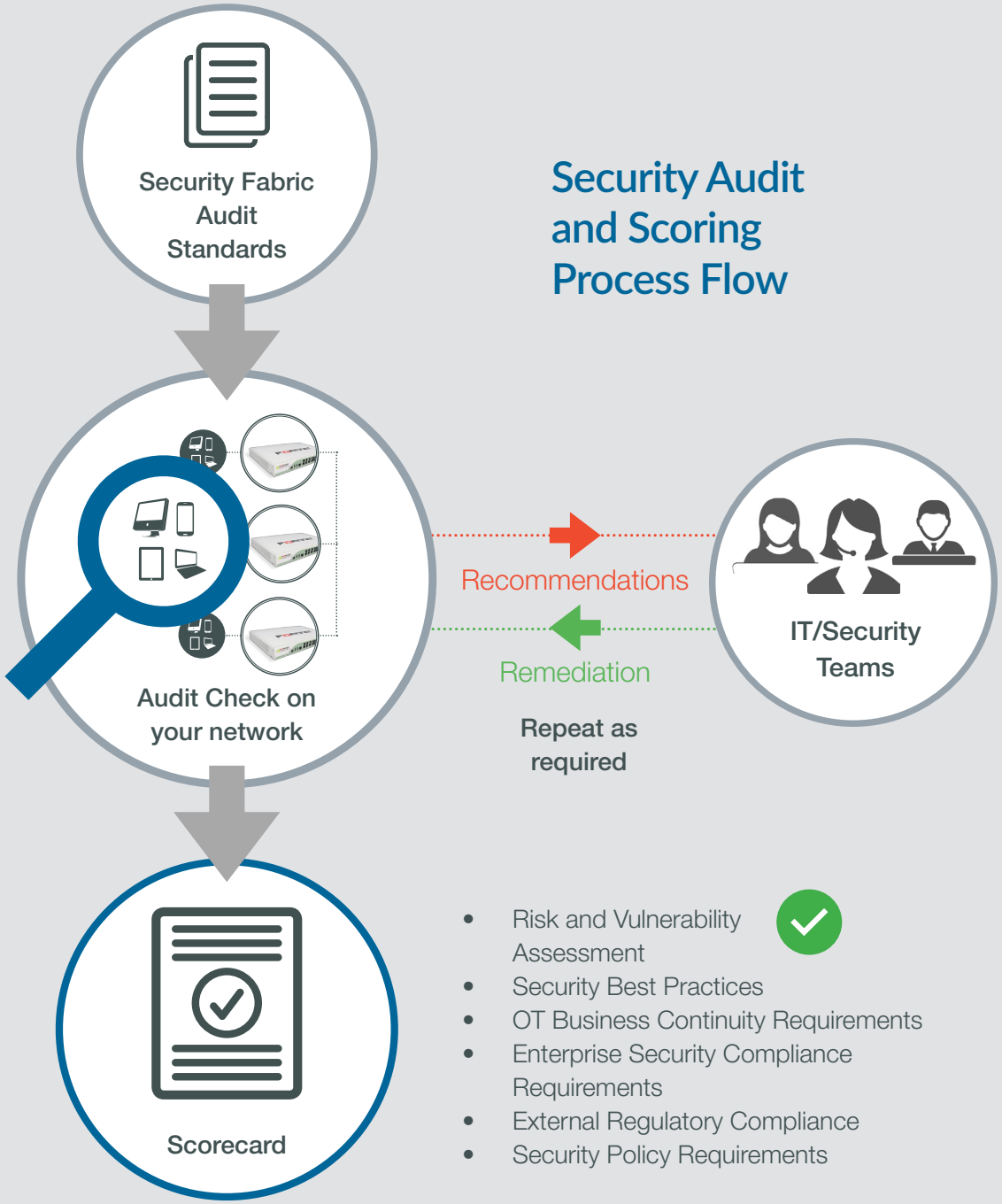
System configurations and policies need to be dynamically changed and enforced, as the complex enterprise network shifts to meet evolving business needs. As a result, security measures and countermeasures need to be provisioned and tuned in a rapid manner which adds to the ongoing pressure on network and security teams. Inevitable errors and misconfigurations are introduced, and lead to failure to provide the trust and assurance that critical assets are being protected.
Based on Security Best Practices and Standards, the capabilities of the Security Fabric can be further leveraged through the Security Fabric Audit and Scoring feature. The feature provides a mechanism to continually assess the Security Fabric, validate configurations are working effectively, and provide awareness of risks and vulnerabilities that may impact daily business operations.

The diagram below shows the audit check and score reporting process flow. The Security Fabric Audit checks are performed on the Security Fabric enabled network and provide scoring and recommendations to operations teams. The Score Card can be used to gauge adherence to various internal and external organizational policy, standards and regulation requirements.

Key features

- Provides up to date risk and vulnerability data in the context of what is important to the business.
- Network and security teams can coordinate and prioritize fixes in a timely manner.
- As Security Fabric features and security audit checks are updated to match evolving vulnerability exploits and attacks, Security and Network teams can identify opportunities to improve systems configurations and automate processes. Resulting in improved network and security operations.
- Helps to keep pace with evolving compliance and regulatory standards

Security Audit and Scoring Process Flow



- Risk and Vulnerability Assessment
- Security Best Practices
- OT Business Continuity Requirements
- Enterprise Security Compliance Requirements
- External Regulatory Compliance
- Security Policy Requirements

This structured approach for configuration monitoring and tuning brings additional value to other critical processes.

- Supports quicker business decisions and remediation in data breach situations.
- The status of 3rd party asset compliance can be monitored to ensure they are adhering to Enterprise Security Policies.
- Risk management teams can proactively monitor the status of security controls against compliance and regulatory standards.
- Brings value to Operations Teams (OT), through early awareness of potentially non-compliant assets, unstable system configuration states, and data flow anomalies.

4 Recommended Security Best Practices

These practices and standards and are intended to guide customers to design, implement and continually maintain a target Security Fabric security posture suited for their organization. The Security Fabric is fundamentally built on security best practices and by running these audit checks, security teams will be able to identify critical vulnerabilities and configuration weaknesses in their Security Fabric setup, and implement best practice recommendations.

The following security checks are currently available as of FortiOS 5.6. Additional security checks and associated recommendation will be added with future FortiOS releases.

FIRMWARE AND SUBSCRIPTIONS (FS)

Maintaining the latest software, firmware and updates on systems ensures the network is operating effectively and maintains the organization target security posture. Performing regular system configuration checks and updates allows optimal performance of the network and security devices' intended functions.

FSBP ID (FORTINET SECURITY BEST PRACTICES)	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
FS01	**Compatible Firmware.** Ensure that the latest compatible software and firmware is installed on all members of the Security Fabric.	From the Security Fabric root, verify that all firewalls in the Security Fabric are running a version of firmware that is compatible with the Security Fabric root. From the Security Fabric root, verify that all access layer devices (Wireless & Switch) are running a version of firmware that is recommended for the firewall that they are managed by.	For any firewalls in the Security Fabric which are not running a compatible version of firmware with the Security Fabric root, upgrade them to a version of firmware that is compatible with the Security Fabric root. For any access layer devices in the Security Fabric which are not running the recommended version of firmware, upgrade them to the recommended version of firmware. Use the published Security Fabric document to validate compatible firmware versions
FS02	**Vendor Support.** Ensure a current support contract with the vendor is in place to obtain the latest security notifications, updates and configuration management best practices.	From the Security Fabric root, verify that every firewall in the Security Fabric has a valid support contract and is registered with the vendor. From the Security Fabric root, verify that every firewall in the Security Fabric has a valid subscription to receive anti-malware and threat security check updates.	If any firewalls in the Security Fabric don't have a valid support/subscription contract or aren't registered with the vendor, then contact the vendor support center to renew/update the support and subscriptions contracts.

NETWORK DESIGN AND POLICIES (ND)

Design a business and risk driven network security architecture to ensure that only authorized business users and traffic are permitted to access network resources. Configuration design should take in account enterprise security and compliance requirements, as well as industry accepted standards for enterprise security.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
ND01	**Unauthorized access layer devices.** All access layer devices such as wireless access points and network switches should be identified and validated. Unauthorized devices should be immediately disabled.	From the Security Fabric root, verify that every access layer device detected behind a firewall in the Security Fabric is authorized to communicate with the firewall, or explicitly disabled from doing so.	Review the unauthorized access layer devices to determine if they should join the Security Fabric, and if so, authorize them from the Security Fabric root. For any unauthorized access layer devices which should not be part of the Security Fabric, explicitly disable them so that no communication takes place. Continue to log and monitor for unauthorized communication to the Security Fabric. Periodically review the logs for persistent traffic from unauthorized devices.
ND02	**Secure Wireless Connections.** Wireless networks should not permit insecure protocols such as WEP or other less secure algorithms.	***Future Release Implementation***	
ND03	**Review unused policies.** All firewall policies should be reviewed every 3 months to verify the business purpose. Unused policies should be disabled and logged.	From the Security Fabric root, verify that every firewall in the Security Fabric has no configured policies which have not forwarded/blocked any traffic in the last 90 days.	Review the policies to determine if they serve a valid business purpose. If not, remove and log the policies from the firewall. Each policy and log entry should include a business and technical owner. Review all policies on a quarterly basis or monthly if frequent policies changes are required.
ND04	**Segregation of Traffic.** Separate servers from end user devices.	From the Security Fabric root, verify that every firewall in the Security Fabric has no servers detected in a segment that also contains end user devices.	End user devices should be separated from internal servers by placing them in a different segment from the server. Firewall interfaces should be labeled with a Security Profile and business purpose description. Publicly accessible servers should be placed behind an interface which is classified as "DMZ" to limit the inbound traffic to only those authorized servers.
ND05	**VLAN Change Management.** VLAN changes should be updated to all firewalls in the Fabric.	From the Security Fabric root, identify any interfaces on a Security Fabric firewall that are directly connected to 3rd party switches.	Any changes to internal VLAN configurations on 3rd party switches must be manually updated on any applicable firewalls in the security fabric. Updates can be automated by replacing the 3rd party switch with a FortiSwitch and attaching it to a suitable firewall though a dedicated switch management port. All VLAN and port assignments on that switch can be performed from within Fabric and then updated to all firewall members.

NETWORK DESIGN AND POLICIES (ND)

Design a business and risk driven network security architecture to ensure that only authorized business users and traffic are permitted to access network resources. Configuration design should take in account enterprise security and compliance requirements, as well as industry accepted standards for enterprise security.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
ND06	**Third Party Router & NAT Devices.** Third party router or NAT devices should be detected in the network.	From the Security Fabric root, identify third party router or NAT devices that are detected on any "LAN" or "DMZ" segments for every firewall in the Security Fabric.	For any 3rd party router or NAT devices that are detected, ensure they are compatible with the Security Fabric in order to provide greater visibility and control user and device traffic.
ND07	**Device Discovery.** Ensure that all systems are detected and logged on internal networks, including DMZ.	From the Security Fabric root, verify that for every firewall in the Security Fabric, any network interfaces classified as "LAN" or "DMZ" has device identification enabled, so that network topology and device movement can be monitored and reported.	For any "LAN" or "DMZ" segments which do not identify and log connected systems, update the configuration by enabling device detection on each interface of each member of the Security Fabric.
ND08	**Interface Classification.** All network interfaces should be assigned a defined and configured based on the security risk profile of the segments and systems being protected.	From the Security Fabric root, verify that for every firewall in the Security Fabric, all network interfaces are classified as either "WAN", "LAN", or "DMZ".	All interfaces should be defined according to the security profile desired for the protection of the systems placed behind them, and labelled according to the business function those systems serve. For each interface on each firewall in the fabric, assign the appropriate security profile ("WAN", "LAN" or "DMZ") and label its business function using the Alias description.
ND09	**Detect Botnet Connections.** Ensure all networks including wired and wireless access points are configured to detect Botnet activity, including any similar suspicious traffic entering and leaving the network.	From the Security Fabric root, verify that for every firewall in the Security Fabric, all network interfaces classified as "WAN" are configured to detect outgoing botnet connections.	Enable the botnet detection and blocking of those Command and Control connections on the "WAN" interface to protect the endpoint and segment from being further compromised. Enable logging and monitoring on those interfaces, and review WAN traffic logs on a regular basis to look for suspicious patterns and external IP addresses.

NETWORK DESIGN AND POLICIES (ND)

Design a business and risk driven network security architecture to ensure that only authorized business users and traffic are permitted to access network resources. Configuration design should take in account enterprise security and compliance requirements, as well as industry accepted standards for enterprise security.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
ND10	**Explicit Interface Policies.** Security policies should permit only authorized least privilege and least required traffic to/from authorized systems.	From the Security Fabric root, verify that for every firewall in the Security Fabric, all configured firewalls policies do not permit traffic to and from multiple interfaces.	Firewall policies should be as explicit as possible when defining how traffic can flow through the firewall. Any policies that are configured with multiple source or destination interfaces should be broken up into individual policies which match specific traffic to and from single interfaces only.
ND11	**Secure Remote Access.** All remote access included site-to-site and personal VPN should require at a minimum 2-Factor authentication.	***Future Release Implementation***	
ND12	**Double-NAT.** Identify if the Security Fabric is performing Network Address Translation multiple times to any traffic pathway.	***Future Release Implementation***	

FABRIC SECURITY HARDENING (SH)

Vendor default configurations should be removed, including all default accounts, passwords and management settings. All unnecessary and insecure services and protocols should be disabled. Only business justified services and protocols should be permitted, logged and reviewed on a regular basis.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
SH01	**Unsecure Management Protocols.** All unsecure and non-business justified firewall management protocols should be removed.	From the Security Fabric root, verify that for every firewall in the Security Fabric, an administrator can connect and manage the firewall through encrypted protocols only.	Disable any unsecure protocols such as TELNET or HTTP that are allowed for firewall management purposes. Limit the number of Management Interfaces on each firewall. Enable only secure encrypted management protocols such as HTTPS or SSH.
SH03	**Valid HTTPS Certificate - Administrative GUI.** The administrative GUI should not be using a default built-in certificate.	From the Security Fabric root, verify that for every firewall in the Security Fabric, the HTTPS administrative interface used to manage the firewall is not using a default (factory provided) SSL/TLS certificate.	Acquire a certificate from a trusted authority and configure the administrative HTTPS GUI interface on the firewall to use it.
SH04	**Valid HTTPS Certificate - SSL-VPN.** SSL-VPN should not be using a default built-in certificate.	From the Security Fabric root, verify that for every firewall in the Security Fabric, SSL-VPN is not using a default (factory provided) SSL/TLS certificate.	Acquire a certificate from a trusted authority and configure SSL-VPN on the firewall to use it, in place of the default certificate.
SH05	**Administrator Password Policy.** A strong password policy including upper, lower alphanumeric characters and at least 8 characters in length should be in place.	From the Security Fabric root, verify that every firewall in the Security Fabric has a strong password policy in place for administrators.	Enable a strong password policy for firewall administrators. Align the policy and its management with the established corporate security policy for critical systems. This should include limiting administrator access to high trust individuals, enforcing unique username and passwords and safekeeping of backup/recovery administrator accounts.

FABRIC SECURITY HARDENING (SH)

Vendor default configurations should be removed, including all default accounts, passwords and management settings. All unnecessary and insecure services and protocols should be disabled. Only business justified services and protocols should be permitted, logged and reviewed on a regular basis.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
SH06	**Potentially Insecure Policies.** Firewall policies should permit only the least required traffic specific for the business function purposes.	***Future Release Implementation***	
SH07	**Illogical Policies.** Firewall policies should permit only specific limited traffic for the business function purposes.	***Future Release Implementation***	
SH08	**Fabric Policy Consistency.** All fabric members should be running policies that enforce consistent security measures	***Future Release Implementation***	

ENDPOINT MANAGEMENT (EM)

All end user and server systems should comply with security and acceptable use policies, to ensure that users and applications activity are monitored and prevented from connecting to unauthorized and unsafe resources. Only authorized applications should be running on end user and server systems.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
EM01	**Endpoint Registration and Vulnerabilities.** The fabric should be aware of any endpoints that may be affected with malicious software.	From the Security Fabric root, for every firewall in the Security Fabric, determine if any endpoint devices are detected having critical vulnerabilities.	Endpoint protection software should be configured to protect endpoint devices and connected to a firewall for vulnerability status maintenance. All devices should be routinely scanned and resolved of any critical and high vulnerabilities immediately (1-2 days). Medium vulnerabilities should be address within 5-10 days. However other mitigation strategies, such as quarantine and network segregation with detailed logging and monitoring, could be considered as compensating controls, if applying security patches or updates is not business feasible.
EM02	**Endpoint Compliance.** Endpoints should be verified for conformance to corporate network security and acceptable use policies. Endpoints should not be permitted to access critical network resources until compliance has been verified.	From the Security Fabric root, verify that for every firewall in the Security Fabric, any endpoint devices detected behind a "LAN" classified interface are validated against a set of security conformance specifications via ATP endpoint protection software that directly communicates with the firewall.	Install endpoint protection software on any endpoint devices, and have those endpoints register with the firewall so that they may be checked for conformance, and report any detected vulnerabilities to the firewall. Only "Compliant" end points should be permitted to access network resources.

THREAT AND VULNERABILITY MANAGEMENT (TV)

All network and user devices should be scanned for weaknesses on a regular basis to detect and prevent current and evolving malicious software threats.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
TV01	**Advanced Threat Protection (ATP).** Suspicious files should be redirected to a Sandbox environment, where it can be safely inspected and verified for malicious content.	From the Security Fabric root, verify that for every firewall in the Security Fabric, an anti-malware profile is configured to send any suspicious files to a sandbox environment for further analysis.	Enable the Security Fabric Anti-virus Security Feature, and ensure a valid Sandbox subscription is enabled. Enable the appropriate Anti-Virus profile Inspection Options based on the corporate security policy for file and executable handling.
TV02	**Endpoint quarantine**	*Future Release Implementation*	
TV03	**Network Anti-Virus**	*Future Release Implementation*	
TV04	**Host based Intrusion Prevention.**	*Future Release Implementation*	
TV05	**Protection from Malicious websites**	*Future Release Implementation*	
TV06	**Detect malicious applications.**	*Future Release Implementation*	
TV07	**UTM Inspection Optimization**	*Future Release Implementation*	

AUDIT LOGGING AND MONITORING (AL)

All user and traffic activity should be tracked and verified based on business priorities basis. Regulatory and other standards require specific types of logs and audit evidence to be collected over a specified period of time in order to demonstrate conformance with those requirements.

FSBP ID	SECURITY CONTROL	TESTING PROCEDURES	RECOMMENDATION
AL01	**Centralized Logging & Reporting.** Logging and reporting should be centralized.	From the Security fabric root, verify that every firewall in the Security Fabric is sending logs to a centralized logging device within the Security Fabric.	Configure each member of the Security Fabric to send all system, traffic, and security traffic logs to a centralized location for analysis and reporting. Centralized logging and analysis reduces administrator effort in manually collecting and merging logs. Often logging servers such as FortiAnalyzer and FortiSIEM have automated and built-in capabilities to perform quicker processing and reporting based on the desired security or network analysis objective.
AL02	**Look for IOC from historical logs.**	***Future Release Implementation***	